

<b>Notice of Allowability</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/674,362	TAKASE, MASAAKI	
	Examiner Thomas R. Peeso	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS. This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to application papers filed.

2.  The allowed claim(s) is/are 1-29 (renumbered).

Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)  All    b)  Some\*    c)  None    of the:

1.  Certified copies of the priority documents have been received.

2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.

3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.

(a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached  
1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.

(b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of  
Paper No./Mail Date \_\_\_\_\_.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- 1.  Notice of References Cited (PTO-892)
- 2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3.  Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date 28Aug2006, 30Sep2003
- 4.  Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
- 5.  Notice of Informal Patent Application
- 6.  Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
- 7.  Examiner's Amendment/Comment
- 8.  Examiner's Statement of Reasons for Allowance
- 9.  Other \_\_\_\_\_

Thomas R Peeso  
Primary Examiner  
Art Unit: 2132

## REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance:

Applicant has claimed uniquely distinct features in the instant invention which are not found in the prior art, either singularly or in combination. invention,

According to the present invention, the key exchange proxy network system includes a key exchange proxy unit performing, as proxy for the terminal unit,a key exchange processing against the opposite terminal unit to perform encryption communication between the terminal units. The key exchange proxy unit includes; a message reception section accessed by the terminal unit, and receiving the message from service control unit transferring the message received from either the terminal unit or the opposite terminal unit; a protocol control section which exchanges key exchange messages with the opposite terminal unit, and determines the key, when the message received by the message reception section is the key exchange message; and a message transmission section which transmits the key determined by the protocol control section to the service control unit as message including the key.

According to the present invention, there is provided a key exchange proxy method applicable for a key exchange proxy network system having a key exchange proxy unit. Here, the key exchange proxy unit performs, as proxy for a first terminal unit, a key exchange processing to be performed between the first terminal unit and a second terminal unit for encryption communication. The key exchange proxy method includes; in the service control unit, transferring a key

exchange message transmitted from either the first terminal unit or the second terminal unit to the key exchange proxy unit; in the key exchange proxy unit, generating the key exchange message to be exchanged between the first terminal unit and the second terminal unit, and transmitting the generated key exchange message to the service control unit; in the service control unit, transferring the key exchange message to the second terminal unit; in the key exchange proxy unit, transmitting a message including the key determined by exchanging the key exchange messages to the service control unit; and in the service control unit transferring to the first terminal unit the message including the key received from the key exchange proxy unit.

According to the present invention, the key exchange message transmitted from either the first terminal unit or the second terminal unit to the service control unit is transferred to the key exchange proxy unit by the service control unit. Thereafter, the key exchange processing is performed between the key exchange proxy unit and the second terminal unit, and a key necessary for the encryption communication is determined- The determined key is transmitted to the first terminal unit.

Thus, according to the present invention, the first unit can obtain the key necessary for the necessary terminal encryption communication without performing processing for the key exchange and the key determination- As a result, it becomes possible to reduce the load of the first terminal unit. Further,

the service control unit transfers the key exchange message received from either the first terminal unit or the second terminal unit to the key exchange proxy unit. Therefore, it is merely necessary for the first terminal unit to recognize the destination address of the second terminal unit. Also, it is merely necessary for the second terminal unit to recognize the destination address of the first terminal unit. Accordingly, the proxy for the key exchange processing can be achieved upon a key exchange request from whichever terminals, either the first terminal unit or the second terminal unit.

According to the present invention, there is provided a service control unit which is accessed by a terminal unit and transfers a message from any one of the terminal unit, a key exchange proxy unit performing a key exchange processing as proxy for the terminal unit and the opposite terminal unit performing encryption communication with the terminal unit. The service control unit includes; a message reception section receiving a message from the terminal unit, the key exchange proxy unit, or the opposite terminal unit; a protocol control section which retains a data for deciding whether a message received by the message reception section is a key exchange message or a message including a key, decides whether the reception message is the key exchange message or the message including the key based on the data determines the key exchange proxy unit as transfer address when the reception message is a key exchange message received from either the terminal unit or

the opposite terminal unit, determines the opposite terminal unit as transfer address when the reception message is a key exchange message received from the key exchange proxy unit, and determines the terminal unit as transfer address when the reception message is a message including the key; and a message transmission section transmitting the reception message to the transfer address determined by the protocol control section.

According to the present invention, the key exchange proxy unit performing, as proxy for the terminal unit, a key exchange processing against the opposite terminal unit to perform encryption communication between the terminal units. The key exchange proxy unit includes; a message reception section which is accessed by the terminal unit and receives the message from service control unit transferring the message received from either the terminal unit or the opposite terminal unit; a protocol control section which exchanges key exchange messages with the opposite terminal unit, and determines the key, when the message received by the message reception section is the key exchange message and a message transmission section which transmits the key determined by the protocol control section to the service control unit as message including the key.

According to the present invention, the terminal unit accesses a service control unit in a communication network, and performs encryption communication with the opposite terminal unit. The terminal unit includes; an encryption process

management section which retains a first data specifying a condition of communication requiring encryption and a second data including a key for use in the encryption, decides whether encryption is required for the communication with the opposite terminal unit based on the first data, and decides whether the key required for the encryption is existent in the second data; a message transmission section which transmits a key exchange message to the opposite terminal unit through the service control unit, when the encryption process management section decides that the encryption is required and that the key required for the encryption is not existent; and a message transmission section which receives the message including the key determined between the key exchange proxy unit in the communication network and the opposite terminal unit from the service control unit.

These features are not found or suggested in the prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas R. Peeso whose telephone number is 571 272-3809. The examiner can normally be reached on Mon.-Fri, 7:00 a.m. to 3:30 p.m. The central fax number for the office is 571 273-8300.

Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571 272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Thomas R. Peeso  
Primary Examiner

31 December 2006